«Меры защиты от преступлений, совершаемых с использованием информационно - коммуникационных технологий»

В нынешний период банковская система все больше уделяет внимание упрощающим жизнь человека высоким технологиям, активно внедряя их в различные операционные процессы для взаимодействия финансового учреждения с многочисленными клиентами. Наиболее популярны телефонные приложения «СбербанкОнлайн», «ВТБОнлайн» и прочие, с помощью которых можно в любое время суток осуществлять банковские операции, оплатив, например, через личный кабинет с помощью банковской карты любой товар в интернет-магазинах. Вместе с тем усиливающаяся информатизация современного общества имеет и негативные последствия, заключающиеся в появлении и росте особых разновидностей правонарушений, злоумышленники, в свою очередь, не стоят на месте. Одна из таких групп преступных посягательств выражается в совершении различных корыстных действий (бездействия) в сферах ИТТ с применением компьютерной информации, электронных (цифровых) технологий и т.п.

Чтобы не стать жертвой преступников, использующих ИКТ, применяйте эти простые правила:

- не сообщайте свои персональные данные, а также банковских карт и счетов третьим лицам, даже если неустановленное лицо представилось сотрудником банка, прекратите разговор и обратитесь в банк лично либо по телефону горячей линии;

- не выполняйте указания неизвестных лиц по вводу каких-либо команд и символов в телефоном режиме, а также с использованием банкомата;

-не перечисляйте денежные средства неизвестным лицам, представляющимся знакомыми ваших родных, сотрудниками правоохранительных органов (положите трубку и позвоните лицу, который по словам неизвестного попал в беду/нуждается в помощи);

- прежде чем приобретать какой-либо товар или услугу с использованием сети Интернет, ознакомьтесь с отзывами, оставленными ранее покупателями/клиентами;

- при вводе пин-кода банковской карты закрывайте его рукой, не храните пин-код совместно с банковской картой.

«Преступления в сфере информационных технологий»

Преступления в сфере информационных технологий включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации.

По Уголовному кодексу Российской Федерации преступлениями в сфере компьютерной информации являются:

— неправомерный доступ к компьютерной информации (ст. 272 УК РФ),

—создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ),

— нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия.

«Механизмы противодействия интернет-мошенничеству»

В настоящее время банковская система все больше уделяет внимание упрощающим жизнь человека высоким технологиям, активно внедряя их в различные операционные процессы для взаимодействия финансового учреждения с многочисленными клиентами. Наиболее популярны телефонные приложения «СбербанкОнлайн», «ВТБ-Онлайн» и прочие, с помощью которых можно в любое время суток осуществлять банковские операции, оплатив, например, через личный кабинет с помощью банковской карты любой товар в интернет-магазинах.

Вместе с тем усиливающаяся информатизация современного общества имеет и негативные последствия, заключающиеся в появлении и росте особых разновидностей правонарушений, злоумышленники, в свою очередь, не стоят на месте.

Одна из таких групп преступных посягательств выражается в совершении различных корыстных действий (бездействия) в сферах ИТТ с применением компьютерной информации, электронных (цифровых) технологий и т.п. Чтобы не стать жертвой преступников, использующих ИКТ, применяйте эти простые правила:

– не сообщайте свои персональные данные, а также банковских карт и счетов третьим лицам, даже если неустановленное лицо представилось сотрудником банка, прекратите разговор и обратитесь в банк лично либо по телефону горячей линии;

– не выполняйте указания неизвестных лиц по вводу каких-либо команд и символов в телефоном режиме, а также с использованием банкомата;

–не перечисляйте денежные средства неизвестным лицам, представляющимся знакомыми ваших родных, сотрудниками правоохранительных органов (положите трубку и позвоните лицу, который по словам неизвестного попал в беду/нуждается в помощи);

– прежде чем приобретать какой-либо товар или услугу с использованием сети Интернет, ознакомьтесь с отзывами, оставленными ранее покупателями/клиентами;

– при вводе пин-кода банковской карты закрывайте его рукой, не храните пин-код совместно с банковской картой.

«Хищение, совершенное с использованием современных информационно-коммуникационных технологий»

Хищение, совершенное с использованием современных информационно-коммуникационных технологий является общественно опасным деянием, причиняющим значительный имущественный вред гражданам. Наблюдается значительный рост преступлений, связанных с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций, совершаемых в виде дистанционного мошенничества.

Злоумышленники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Они преследуют цель – получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных о банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками или представителями правоохранительных органов.

В подавляющем большинстве случаев преступники используют следующие основные схемы обмана. Так, злоумышленник звонит или отправляет смс-сообщение на телефон, сообщая что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника.

Может поступить звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет мошенника.

Потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ. В таких случаях важно быть внимательным и не использовать непроверенные сайты, в том числе сайты-двойники.

При возникновении подобных ситуаций необходимо оперативно самостоятельно связаться с оператором банка, сотовой связи с целью блокировки карты, номера телефона, отключения услуг и т.д. Данные действия способствуют незамедлительному установлению злоумышленника и предотвращению совершения преступления.

Важно помнить! Ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код.

Исключите разговоры с неизвестными лицами по поводу состояния Ваших банковских счетов. При необходимости получить кредит или воспользоваться иными банковскими услугами обращайтесь непосредственно в офисы банковских организаций или пользуйтесь официальными сайтами и приложениями проверенных банков.

«Преступления в сфере ИТТ в отношении несовершеннолетних».

В соответствии с распоряжением Президента Российской Федерации Генеральному прокурору Российской Федерации поручено подписание Конвенции ООН против киберпреступности.

Государства-члены ООН в декабре 2024 года приняли первую юридически обязывающую Конвенцию по киберпреступности, которая является универсальным международным договором в борьбе с противоправными деяниями в цифровой сфере.

25 октября 2025 года Генеральный прокурор России Александр Гуцан, а также уполномоченные представители 71 государства подписали Конвенцию ООН против киберпреступности.

Документ предусматривает оказание оперативной помощи для ускорения расследования киберпреступлений, процедур экстрадиции, изъятия доходов от преступной деятельности и возврата активов, защиты детей от сексуального насилия с использованием IT, помощи пострадавшим от действий киберпреступников, а также обязанность стран-участниц разрабатывать программы компенсации ущерба жертвам мошенничества, программы реабилитации и восстановления пострадавших.

Такое сотрудничество позволит объединить усилия правоохранительных органов различных стран в области информационной безопасности в интересах всего мирового сообщества.

Кибергруминг — это современное понятие интернет преступлений эротического характера, совершенного против несовершеннолетних детей в процессе доверительного общения в сети Интернет.

Жертвой интернет злоумышленника может стать любой, но чаще это дети, не достигшие совершеннолетнего возраста, которые более подвержены манипуляциям. Бывают случаи, когда ребенок страдает от дефицита внимания и хочет восполнить недостаток заинтересованности родителей в его жизни. Находясь в такой обстановке, он может начать воспринимать любое положительное внимание к себе, как праздник, не подозревая опасности.

Любопытство и недостаток жизненного опыта могут сделать ребенка легко доступной жертвой преступления. Пытаясь узнать больше об интимной жизни, вопреки страху родительского наказания, дети доверяются незнакомцам из интернета, которые подробно рассказывают об интимных отношениях и предлагают вступить в половую связь.

Как все начинается? Злоумышленник знакомится с ребенком в социальных сетях, мессенджерах или на форумах, притворяясь сверстником и, скрывая свой истинный возраст, начинает самое простое общение. Параллельно он узнает личную информацию о ребенке, об отношениях в семье, где проживает, с кем общается, какой адрес школы или дома, номер мобильного телефона, другие профили в социальных сетях.

Наладив доброжелательное общение, лжедруг приглашает на видеозвонки, личные встречи, выманивая интимные изображения несовершеннолетнего. С помощью видеозвонков и отправленных фотографий создаётся порнографический материал, который в дальнейшем может незаконно

распространяться и использоваться, как инструмент шантажа. Дети не знают, что делать в таких ситуациях, поэтому продолжают поддаваться на манипуляции.

Как понять, что ваш ребенок в опасности? Он становится более скрытным и замкнутым. Пытается скрыть такого рода переписку, резко реагирует, если родители забирают гаджеты, начинает просить больше денег на «карманные расходы». Он может удалять свои социальные сети и просить поменять ему номер телефона. Эти проблемы могут привести к снижению его успеваемости в школе и он перестает общаться с друзьями.

Если ваш ребенок оказался в такой ситуации, постарайтесь сохранять спокойствие и действовать последовательно. Сохраните все фотографии, адреса, скрины переписок и другие улики, обратитесь в правоохранительные органы. Знайте, такие деяния против половой неприкосновенности несовершеннолетних и общественной нравственности влекут уголовную ответственность вплоть до 20 лет лишения свободы.

В такие моменты детям нужна максимальная поддержка, а не осуждение за проступок. Не нужно стыдить, осуждать или обвинять ребёнка. Лучше сказать, что вы его любите и поможете ему. Контролируйте свои негативные эмоции: страх, обиду, гнев. Они усиливают тревогу и переживания ребёнка. Нужно быть готовым к тому, что у ребёнка могут появиться эмоциональные и поведенческие проблемы во взаимоотношениях или в учёбе. Нужно помочь ему вернуться к ежедневным делам, чаще разговаривать й слушать его. Если вы чувствуете, что ребенок и вы сами не справляетесь с этой ситуацией самостоятельно, следует обратиться за психологической поддержкой.

Чтобы ваш ребенок не стал жертвой такого рода преступления, выстраивайте с ним доверительные отношения, проявляйте заботу, оказывайте поддержку, предупреждайте об опасности общения с незнакомыми людьми, своим примером показывайте, как интересно можно проводить время без гаджетов.

Помните, что родители несут ответственность за жизнь и здоровье ребенка, его нравственное развитие.

«Хищения, совершенные в сфере ИТТ »

Под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (п. 1 примечаний к ст. 158 УК РФ).

Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение. Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим (п. п. 2, 3 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 “О судебной практике по делам о мошенничестве, присвоении и растрате”, далее – Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48).

Мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

«Как не стать жертвой телефонного мошенничества?»

Если гражданин предполагает, что стал жертвой телефонного мошенничества, ему необходимо обратиться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника. Если гражданин, к примеру, совершил перевод денежной суммы по мобильной сети, то принятие оператором экстренных мер может позволить заблокировать перевод и вернуть деньги.

Для того чтобы не стать такой жертвой, необходимо следовать определенным правилам. Например:

– если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу, идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

– нельзя сообщать по телефону личные сведения или данные банковских карт, которые могут быть использованы злоумышленниками для неправомерных действий;

– нельзя перезванивать на номер, если он незнаком, и т.п.

«Уголовная и административная ответственность за телефонное мошенничество»

Телефонное мошенничество в зависимости от размера похищенного и других обстоятельств деяния (например, имеются или отсутствуют признаки преступления) может повлечь административную или уголовную ответственность.

На основании ч. 1 ст. 7.27 КоАП РФ мелкое хищение чужого имущества, стоимость которого не превышает 1 000 руб., путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее 1 000 руб., либо административный арест на срок до 15 суток, либо обязательные работы на срок до 50 часов.

Согласно ч. 2 указанной статьи мелкое хищение чужого имущества стоимостью более 1 000 руб., но не более 2 500 руб. путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее 3 000 руб., либо административный арест на срок от 10 до 15 суток, либо обязательные работы на срок до 120 часов.

Кроме того, на основании ст. 7.27.1 КоАП РФ причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа в размере до пятикратной стоимости причиненного ущерба, но не менее 5 000 руб.

Статья 159 УК РФ предусматривает различные виды наказания за мошенничество в зависимости от конкретных обстоятельств.

Согласно ч. 1 указанной статьи мошенничество наказывается штрафом в размере до 120 000 руб. или в размере заработной платы или иного дохода осужденного за период до 1 года, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет.

Квалифицирующими признаками телефонного мошенничества, к примеру, являются следующие:

– совершение группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину;

– совершение лицом с использованием своего служебного положения, а равно в крупном размере.

«За какие преступления в сфере компьютерной информации предусмотрена конфискация имущества»

С 24 июня 2023 года вступают в силу изменения, внесенные Федеральным законом от 13.06.2023 № 214-ФЗ в статью 104.1 Уголовного кодекса Российской Федерации (конфискация имущества).

С учетом изменений подлежит принудительному безвозмездному изъятию и обращению в собственность государства на основании обвинительного приговора имущество, полученное в результате:

–создания, использования и распространения вредоносных компьютерных программ;

–неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;

–неправомерного доступа к компьютерной информации;

–нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

«Административная ответственность за нарушение законодательства Российской Федерации в области персональных данных при отсутствии признаков уголовно наказуемого деяния»

С 30 мая 2025 года действует Федеральный закон от 30 ноября 2024 года № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», которым внесены изменения в статью 13.11 указанного Кодекса. Ею установлена административная ответственность за нарушение законодательства Российской Федерации в области персональных данных при отсутствии признаков уголовно наказуемого деяния.

Размер административного штрафа за обработку персональных данных в случаях, не предусмотренных законодательством, либо за обработку персональных данных, несовместимую с целями их сбора, для граждан составит от 10 до 15 тыс. руб., для должностных лиц – от 50 до 100 тыс. руб., для юридических лиц – от 150 до 300 тыс. руб. Повторное совершение данного правонарушения лицом, подвергнутым административному наказанию, повлечет наложение административного штрафа на граждан от 15 до 30 тыс. руб., на должностных лиц – от 100 до 200 тыс. руб., на юридических лиц – от 300 до 500 тыс. руб.

Введена административная ответственность операторов при обработке персональных данных.

Невыполнение оператором обязанности по уведомлению уполномоченного государственного органа о намерении осуществлять обработку персональных данных повлечет наложение административного штрафа на граждан от 5 до 10 тыс. руб., на должностных лиц – от 30 до 50 тыс. руб., на юридических лиц – от 100 до 300 тыс. руб.

Ненадлежащее уведомление оператором уполномоченного органа о неправомерной или случайной передаче персональных данных повлечет наложение административного штрафа на граждан от 50 до 100 тыс. руб., на должностных лиц – от 400 до 800 тыс. руб., на юридических лиц – от 1 до 3 млн руб.

Установлена административная ответственность операторов за действия или бездействие, повлекшие неправомерную передачу информации, включающей персональные данные или идентификаторы, то есть уникальные сведения для определения лиц с использованием биометрических персональных данных.

Ответственность начинается с незаконной передачи информации от тысячи до 10 тыс. субъектов персональных данных или от 10 тыс. до 100 тыс. идентификаторов, за что административный штраф составит для граждан от 100 до 200 тыс. руб., для должностных лиц – от 200 до 400 тыс. руб., для юридических лиц – от 3 до 5 млн руб., заканчивается штрафом за незаконную передачу информации о более 100 тыс. субъектов персональных данных или более 1 млн идентификаторов для граждан от 300 до 400 тыс. руб., для должностных лиц – от 400 до 600 тыс. руб., для юридических лиц – от 10 до 15 млн руб. Повторное совершение указанных действий, лицом, подвергнутым административному наказанию, повлечет наложение административного штрафа на граждан от 400 до 600 тыс. руб., на должностных лиц – от 800 тыс. руб. до 1,2 млн руб., для юридических лиц – от 1 до 3 % совокупного размера

суммы выручки за предшествующий год или часть года, в котором совершено правонарушение, или той же части собственных средств кредитной организации, но не менее 20 и не более 500 млн руб.

Также введена ответственность за неправомерную передачу специальной категории персональных данных, биометрических персональных данных, в том числе повторно лицом, подвергнутым административному наказанию.

Особое внимание следует обратить на то, что 50-процентная скидка при быстрой уплате штрафа не применяется по всем составам, предусмотренным статьей 13.11 Кодекса Российской Федерации об административных правонарушениях.

Кроме того, статьей 272.1 УК РФ, введенной Федеральным законом от 30 ноября 2024 года № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», с 11 декабря 2024 года установлена уголовная ответственность занезаконные действия с персональными данными.

В соответствии с ней незаконные использование, передача, сбор и хранение компьютерной информации с персональными данными, полученной путем неправомерного доступа к средствам ее обработки, хранения либо иным незаконным путем, повлекут наказание для лица, совершившего преступление, от штрафа в размере до 300 тыс. руб. до лишения свободы на срок до 4 лет.

За те же деяния в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных и биометрические персональные данные, может быть назначено наказание от штрафа до 700 тыс. руб. до лишения свободы на срок до 5 лет.

При совершении указанных преступлений из корыстной заинтересованности, с причинением крупного ущерба, группой лиц по предварительному сговору, с использованием своего служебного положения наказание составит от штрафа до 1 млн руб. до лишения свободы на срок до 6 лет.

Также предусмотрена уголовная ответственность за подобные преступления, сопряженные с трансграничной передачей компьютерной информации, содержащей персональные данные, и трансграничным перемещением носителей информации с такими данными, а также за их совершение с тяжкими последствиями либо организованной группой.

Одновременно уголовно преследуется создание и обеспечение функционирования информационного ресурса, в том числе в сети «Интернет», заведомо предназначенного для незаконных хранения, передачи, распространения, предоставления, доступа к полученной незаконным путем компьютерной информации, содержащей персональные данные. Подобные действия повлекут наказание от штрафа до 700 тыс. руб. до лишения свободы на срок до 5 лет.

К уголовной ответственности за незаконные действия с персональными данными может быть привлечено любое физическое лицо.

«Введена уголовная ответственность за пропаганду в информационно-телекоммуникационных сетях наркотических средств, психотропных веществ, их аналогов, веществ, используемых при производстве, изготовлении и переработке наркотических сред»

С 01 сентября 2025 года действует Федеральный закон от 08.08.2024 № 226-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации», которым Уголовный кодекс Российской Федерации дополнен статьей 230.3.

Ею установлена уголовная ответственность за пропаганду наркотических средств, психотропных веществ, их аналогов или прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, в информационно-телекоммуникационных сетях, включая сеть «Интернет», совершенную лицом после его привлечения к административной ответственности за аналогичное деяние два раза в течение одного года либо имеющим судимость за совершение преступления, предусмотренного настоящей статьей.

В соответствии с Федеральным законом от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» прекурсоры наркотических средств и психотропных веществ – это вещества, часто используемые при производстве, изготовлении, переработке наркотических средств и психотропных веществ, включенные в Перечень наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, в соответствии с действующим законодательством и международными договорами Российской Федерации, в том числе Конвенцией Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 года.

Административная ответственность за пропаганду наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства, психотропные вещества или их прекурсоры, их частей, содержащих наркотические средства, психотропные вещества или их прекурсоры, либо новых потенциально опасных психоактивных веществ с использованием информационно-телекоммуникационной сети «Интернет» установлена частью 1.1 статьи 6.13 Кодекса об административных правонарушениях Российской Федерации.

Пропагандой является размещение в информационно-телекоммуникационной сети «Интернет», в частности, на видеохостингах, страницах социальных сетей, сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ, их прекурсоров, местах их приобретения, способах и местах культивирования наркосодержащих растений, а также совершение иных действий в целях побуждения интереса у зрителя (читателя) к наркотическим средствам, психотропным веществам и их прекурсорам, способам их употребления, формирования представления о совершении подобных действий для достижения состояния наркотического опьянения как допустимого и желательного.

Например, запрещено законом и является наказуемым размещение в свободном публичном доступе фотографий, изображений, аудио- и видеофайлов, в которых дается положительная оценка наркотикам и

допустимости их употребления, указываются способы употребления наркотических средств, демонстрируются наркотические средства, способы их выращивания, содержатся инструкции по незаконному обороту наркотиков и распространению наркотических средств и психотропных веществ.

Преступления, предусмотренные статьей 230.3 Уголовного кодекса Российской Федерации, будут расследоваться следователями органов внутренних дел Российской Федерации.

За их совершение виновным лицам может быть назначено наказание от штрафа в размере от ста тысяч до трехсот тысяч рублей до лишения свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на тот же срок.

«Прокурор разъясняет: Подписан закон об уголовной ответственности для дропперов»

С 5 июля 2025 года вступили в силу изменения статьи 187 Уголовного кодекса Российской Федерации («Неправомерный оборот средств платежей»).Данные изменения направлены на борьбу с «дропперами» – лицами, которые за вознаграждение предоставляют свои банковские карты и счета для совершения незаконных финансовых операций.Согласно нововведениям статья 187 УК РФ дополнена новыми частями 3-6:Часть 3 предусматривает ответственность лица за передачу из корыстной заинтересованности предоставленных ему оператором по переводу денежных средств электронного средства платежа и (или) доступа к нему другому лицу для осуществления таким лицом неправомерных операций.

В части 4 речь идет об уголовной ответственности лица за осуществление из корыстной заинтересованности неправомерных операций с использованием электронного средства платежа, предоставленного ему оператором по переводу денежных средств, по указанию другого лица и (или) в интересах такого лица.При этом, лицо, являющееся клиентом оператора по переводу денежных средств, впервые совершившее преступление, предусмотренное вышеуказанными частями, освобождается от уголовной ответственности за его совершение, если активно способствовало его раскрытию и (или) расследованию и добровольно сообщило о лицах, совершивших другие преступления с использованием предоставленного ему оператором по переводу денежных средств электронного средства платежа.

К категории тяжких преступлений (лишение свободы до 6 лет) относятся 5 и 6 часть, которые устанавливают ответственность лица за приобретение либо передачу другому лицу из корыстной заинтересованности электронного средства платежа и (или) доступа к нему для осуществления неправомерных операций, совершенные лицом, не являющимся стороной договора об использовании этого электронного средства платежа, заключенного с оператором по переводу денежных средств, либо приобретение таким лицом электронного средства платежа и (или) доступа к нему для последующей их передачи другому лицу из корыстной заинтересованности и за осуществление неправомерной операции с использованием электронного средства платежа, совершенное лицом, не являющимся стороной договора об использовании этого электронного средства платежа, заключенного с оператором по переводу денежных средств, соответственно.

«Прокурор разъясняет: в целях противодействия спам-звонкам и телефонному мошенничеству с 1 сентября 2025 года установлен порядок регулирования массовых телефонных вызовов»

В целях принятия дополнительных мер по борьбе с кибермошенничеством с 1 сентября 2025 года вступили в силу положения статьи 44.1-1 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», которыми предусмотрено право абонента отказаться от получения массовых телефонных звонков.

Такие вызовы теперь должны осуществляться при условии получения предварительного согласия абонента, выраженного его действиями, однозначно идентифицирующими этого абонента и позволяющими достоверно установить его волеизъявление на получение массовых вызовов. Если заказчик массовых вызовов (в случае массовых вызовов по его инициативе) или оператор связи (в случае массовых вызовов по его инициативе) не докажет, что согласие абонента было получено, то массовые вызовы признаются осуществленными без предварительного согласия.

Массовые вызовы по инициативе заказчика массовых вызовов должны производиться на основании договора, заключенного с оператором, абоненту которого предназначены массовые вызовы.

Указанные требования не распространяются на массовые вызовы по инициативе государственных органов и подведомственных им организаций, органов местного самоуправления и подведомственных им организаций, а также иных органов и организаций, перечень которых устанавливается Правительством Российской Федерации.

В свою очередь, абонент в соответствии с требованиями пунктов 222-226 постановления Правительства Российской Федерации от 30.12.2024 № 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте – физическом лице» лично или с использованием сети «Интернет», в том числе системы самообслуживания оператора связи, вправе направить оператору связи отказ от получения массовых вызовов.

Получив отказ гражданина от массовых телефонных вызовов, оператор связи обязан их прекратить на следующий за днем подачи заявления день.

«Прокурор разъясняет: с 30 сентября 2025 г. вводятся правила, приравнивающие предъявление персональных данных в мобильном приложении Единого портала государственных услуг, к оригиналу паспорта».

Возможность предоставления гражданами России сведений, содержащихся в документах, удостоверяющих личность, с использованием информационных технологий была предусмотрена Указом Президента Российской Федерации от 18.09.2023 № 695.

Однако до сентября текущего года конкретные ситуации, в каких случаях это разрешается делать официально не были определены.

В развитие названного Указа Президента постановлением Правительства Российской Федерации от 19.09.2025 № 1443 приняты Правила применения мобильного приложения федеральной государственной информационной системы “Единый портал государственных и муниципальных услуг (функций)”.

Данным нормативным документом уточняется, что мобильным приложением разрешается пользоваться гражданам, достигшим 14-летнего возраста и получившим паспорт Российской Федерации.

Предусматривается поэтапное введение возможности предъявления сведений, заменяющих официальные документы, через мобильное приложение Единого портала госуслуг. Всего таких этапов 6. На первом из них можно будет подтверждать возраст покупателя алкогольной, табачной и никотиносодержащей продукции, безалкогольных энергетических напитков, кальянов и устройств для потребления никотинсодержащей продукции, пиротехнических изделий и сжиженного газа, а также при посещении музея и(или) зрелищного мероприятия, при приеме почтовых отправлений.

В дальнейшем удостоверять личность посредством мобильного приложения можно будет в банках, многофункциональных центрах предоставления государственных услуг, пунктах оказания услуг мобильной связи, при заселении в гостиницы и в других случаях.

В целях удостоверения личности через мобильное приложение необходимо предъявлять свою фотографию, а также генерируемый в автоматическом режиме двухмерный штриховой код (QR-код), который будет считываться специальным техническим устройством, в том числе с использованием технологии NFC.

Чтобы воспользоваться возможностью предъявления персональных данных, удостоверяющих личность, взамен паспорта необходимо пройти процедуру идентификации в многофункциональном центре предоставления государственных и муниципальных услуг с размещением сведений в единой биометрической системе. Гражданам, ранее разместившим свои биометрические персональные данные в государственной единой биометрической системе, в том числе при получении заграничного паспорта, осуществлять заново подтверждение личности не требуется.

«Мошенничество с использованием электронных средств платежа и в сфере компьютерной информации»

В последнее десятилетие в Российской Федерации хищения с использованием средств связи набирают стремительные обороты.

Законодатель, пытаясь сдержать рост указанного вида хищений, реагирует на данную ситуацию. Это подтверждается теми изменениями, которые вносятся в уголовное законодательство. Так, Федеральным законом от 23 апреля 2018 года часть 3 статьи 158 и часть 3 статьи 159.3 УК РФ были дополнены особо квалифицирующим признаком: «деяния, совершенные с банковского счета, а равно в отношении электронных денежных средств». Кроме того, ужесточена санкция за мошенничество с использованием электронных средств платежа: арест на срок до четырех месяцев заменен на лишение свободы на срок до трех лет.

Подчеркивая общественную опасность преступлений, предусмотренных за мошенничество с использованием электронных средств платежа и в сфере компьютерной информации, законодатель снизил пороговое значение крупного размера с одного миллиона пятисот тысяч рублей до двухсот пятидесяти тысяч рублей, особо крупного – с шести миллионов рублей до одного миллиона рублей.

Все рассматриваемые хищения денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, можно разделить на две основные группы:

1) бесконтактные, то есть совершаемые без личностного контакта субъекта с потенциальным потерпевшим (преступления, в которых субъект не контактирует с потерпевшим);

2) контактные, то есть совершаемые посредством установления личностного контакта субъекта с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения).

Также хищения денежных средств можно разделить на следующие виды, это когда:

- субъект осуществляет телефонный звонок от лица вымышленных сотрудников банка или службы безопасности и сообщает о необходимости предоставления информации о номере карты, ее владельце, сроке действия, трехзначном коде, указанном на оборотной стороне карты, в связи с «проведением профилактических работ», «блокированием карты по подозрению в попытке хищения денег» и т.п.;

- субъект просит предоплату за товар или услуги в Интернете;

- субъект сообщает о выигрыше;

- субъект осуществляет телефонный звонок лицу и сообщает, что у его родственника (знакомого) проблемы, например, попал в ДТП, совершил правонарушение и т.п., и предлагает «решить проблему» с помощью внесения на счет злоумышленника определенной денежной суммы.

Следует отметить, что число указанных противоправных деяний продолжает увеличиваться. Высокая степень общественной опасности таких преступлений подтверждается их спецификой - совершить их могут лица, обладающие специальными знаниями и использующие технические средства именно в криминальных целях, что приводит к нарушению не только права собственности, но и банковской тайны.

Прокуратура республики призывает граждан быть бдительными и внимательными.

«О противодействии преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий»

Хищение, совершенное с использованием современных информационно-коммуникационных технологий, является общественно опасным деянием, причиняющим значительный имущественный вред гражданам. Наблюдается значительный рост преступлений, связанных с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций, совершаемых в виде дистанционного мошенничества. Злоумышленники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Они преследуют цель - получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных о банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками или представителями правоохранительных органов.

В подавляющем большинстве случаев преступники используют следующие основные схемы обмана. Так, злоумышленник звонит или отправляет смс-сообщение на телефон, сообщая что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника.

Может поступить звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет мошенника.

Потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ. В таких случаях важно быть внимательным и не использовать непроверенные сайты, в том числе сайты-двойники.

При возникновении подобных ситуаций необходимо оперативно самостоятельно связаться с оператором банка, сотовой связи с целью блокировки карты, номера телефона, отключения услуг и т.д. Данные действия способствуют незамедлительному установлению злоумышленника и предотвращению совершения преступления.

Важно помнить! Ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код. Исключите разговоры с неизвестными лицами по поводу состояния Ваших банковских счетов. При необходимости получить кредит или воспользоваться иными банковскими услугами обращайтесь непосредственно в офисы банковских организаций или пользуйтесь официальными сайтами и приложениями проверенных банков.

«Хищение денежных средств со счетов банковских карт с использованием фишинговых ссылок»

В настоящее время одной из наиболее актуальных проблем являются преступления, совершаемые в сфере (с использованием) ИТТ. Наиболее часто регистрируются преступные деяния, совершенные с использованием сети «Интернет», мобильной связи, компьютерной информации, а также расчетных (пластиковых) карт.

Какие виды и способы хищения являются самыми распространенными?

Распространенным видом преступлений является «телефонное мошенничество», совершенное под видом работников банка, сотрудников правоохранительных органов, медицинских и социальных работников.

Данный вид преступления заключается в том, что злоумышленник вводит гражданина в стрессовую ситуацию посредством телефонного звонка. При этом мошенники используют множество предлогов для обмана, манипулируя, в том числе страхами граждан лишиться накопленных денежных средств.

Хищение денежных средств с утерянных либо украденных банковских карт при наличии пин-кода, либо путем бесконтактной оплаты товаров в торговых объектах.

Хищение денежных средств со счетов банковских карт с использованием фишинговых ссылок.

Преступники навязывают потерпевшим ссылку для оплаты, представляющую собой клон сайта либо форму для ввода реквизитов карты. В случае если потерпевший поверил злоумышленнику и пройдя по ссылке ввел реквизиты своей карты, то его денежные средства списываются на счет мошенников.

Каким образом обезопасить себя от действий преступников?

Во-первых - Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Установите и обязательно обновляйте антивирусные программы, а также определители номеров.

Во-вторых - Никому не сообщайте персональные данные, в том числе пароли и коды доступа. Если есть подозрение, что стали доступны личные данные или реквизиты карты, ее нужно заблокировать и перевыпустить.

В - третьих. При любом подозрительном звонке - свяжитесь с банком по номеру телефона, указанному на официальном сайте, в мобильном приложении или на банковской карте.

Если Вы стали жертвой мошенников – незамедлительно обращайтесь в полицию. В соответствии с уголовно-процессуальным законодательством правоохранительные органы обязаны принять и проверить сообщение о любом совершенном или готовящемся преступлении и в пределах компетенции принять по нему решение в срок не позднее 3 суток со дня его поступления.

По результатам рассмотрения сообщения о преступлении должно быть принято одно из решений, а именно: 1) о возбуждении уголовного дела; 2) об отказе в возбуждении уголовного дела; 3) о передаче сообщения по подследственности, а по уголовным делам частного обвинения – в суд.

Кроме того, любой гражданин может обратиться и в прокуратуру за защитой своих прав, например, если правоохранительные органы отказываются

регистрировать Ваше заявление или по Вашему мнению вынесли неправомерное процессуальное решение по нему.

«О получении статуса блогера»

Активное применение современных видов связи является неотъемлемой характеристикой современности. В настоящее время этот вектор развития общественной жизнедеятельности объективно обуславливает высокий уровень киберпреступности в России в целом, при этом большую часть таких преступлений составляют «дистанционные» мошенничества, совершаемые с использованием средств мобильной связи либо сети «Интернет».

На сегодняшний день на территории Российской Федерации сформировалась судебная практика по взысканию на основании исков потерпевших граждан неосновательного обогащения с непосредственных владельцев счетов, на которые перечислены похищенные денежные средства. Так, согласно положениям статьи 1102 Гражданского кодекса Российской Федерации лицо, которое без установленных законом, иными правовыми актами или сделкой оснований приобрело или сберегло имущество за счет другого лица (потерпевшего), обязано возвратить последнему неосновательно приобретенное или сбереженное имущество (неосновательное обогащение). При этом в соответствии с частью 1 статьи 56 Гражданского процессуального кодекса Российской Федерации обязанность доказать наличие обстоятельств, в силу которых неосновательное обогащение не подлежит возврату, либо то, что денежные средства или иное имущество получены обоснованно и неосновательным обогащением не являются, возлагается на ответчика.

Обозначенная судебная практика позволит потерпевшим от преступлений эффективно защищать свои права, а прежде всего возмещать причиненный ущерб даже при неустановлении лица, виновного в совершенном хищении. Для получения правовой помощи по вопросам противодействия «дистанционным» мошенникам и реализации права на взыскание похищенных денежных средств жители Нашего района вправе обратиться в прокуратуру района.

«Неправомерный доступ к компьютерной информации»

Преступления в сфере информационных технологий включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации.

По Уголовному кодексу Российской Федерации преступлениями в сфере компьютерной информации являются:

— неправомерный доступ к компьютерной информации (ст. 272 УК РФ),

—создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ),

— нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия.

«Оборот фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и фальсифицированных биологически активных добавок с помощью сети Интернет»

Прокуратура разъясняет про преступления с использованием информационных технологий Развитие информационно-телекоммуникационных технологий и увеличение числа преступлений, совершенных с помощью сети Интернет, средств мобильной связи, компьютерных техники и программ, пластиковых карт и иных технологий на базе сети Интернет, потребовало от законодателя усиления уголовно-правовой защиты граждан и организаций. Федеральным законом от 01.04.2020 № 95-ФЗ внесены изменения в статью 238.1 УК РФ, предусматривающую наказание за оборот фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и фальсифицированных биологически активных добавок. Данные действия, совершенные с использованием сети Интернет, переведены из категории средней тяжести в число тяжких преступлений, максимальное наказание за их совершение увеличено с 5 до 6 лет лишения свободы. В 2018 году ужесточена ответственность за совершение краж денежных средств с банковского счета, которые по степени тяжести приравнены к кражам с незаконным проникновением в жилище и караются лишением свободы на срок до 6 лет (пункт «г» части 3 статьи 158 УК РФ).

Ранее законодателем введен специальный состав мошенничества, совершенного с использованием электронных средств платежа (статья 159.3 УК РФ), к которым в соответствии с Федеральным законом «О национальной платежной системе» относятся средства и (или) способы, позволяющие составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, иных технических устройств. При этом неправомерный оборот данных средств платежа (незаконное их изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт) относится к тяжким преступлениям и влечет наказание до 6 лет лишения свободы (часть 1 статьи 187 УК РФ).

В отдельный состав преступления выделено мошенничество в сфере компьютерной информации (статья 159.6 УК РФ), связанное с хищением чужого имущества путем получения доступа к компьютерной системе и совершения определенных действий (ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства).

В соответствии с Постановлением Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48, в случае совершения данного деяния посредством неправомерного доступа к компьютерной информации либо создания, использования и распространения вредоносных компьютерных программ оно подлежит квалификации по совокупности преступлений, предусмотренных статьей 159.6 УК РФ и соответствующей статьей главы 28 УК РФ «Преступления в сфере компьютерной информации».

Повышенная уголовная ответственность также установлена за совершение с использованием сети Интернет таких преступлений, как доведение до самоубийства (статья 110 УК РФ), вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни (статья 151.2 УК РФ), сбыт наркотических средств, психотропных веществ или их аналогов (статья 228.1 УК РФ), незаконные изготовление и оборот порнографических материалов (статья 242 УК РФ), публичные призывы к осуществлению террористической и экстремистской деятельности (статьи 205.2 и 280 УК РФ), и ряда других преступлений. Защита прав и законных интересов гражданина в первую очередь зависит от его ответственного отношения к использованию достижений научно-технического прогресса и соблюдения законодательства.

«Неправомерный доступ к компьютерной информации»

Уголовная ответственность за преступления в сфере компьютерной информации предусмотрена главой 28 УК РФ, содержащей три статьи.

Так, статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Впервые в уголовном законодательстве Российской Федерации Федеральным законом от 07.12.2011 N 420-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" в примечании к ст. 272 УК РФ дано понятие компьютерной информации, как предмета преступления, к которому теперь относятся сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Общим объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. В ч. 3 ст. 272 УК РФ указан дополнительный объект преступления – общественные отношения, обеспечивающие интересы службы.

Диспозиция ч. 1 ст. 272 УК РФ в предыдущей редакции от 07.03.2011 была изложена следующим образом: "Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети". В действующей редакции от 07.12.2011 ч. 1 ст. 272 УК РФ изложена следующим образом: "Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации".

Несомненно, законодатель внес данные изменения, чтобы решить ряд проблем, возникающих в правоприменительной практике. Например, при рассмотрении дел указанной категории суды зачастую сталкивались с трудностями, когда неправомерный доступ осуществлялся к устройству, не подпадающему под определение ЭВМ, но по своим свойствам и функциям фактически не уступающему ЭВМ по возможности хранения и обработки информации (мобильные телефоны, смартфоны, карманные персональные компьютеры).

Объективная сторона состава преступления включает в себя: действие, состоящее в неправомерном доступе к охраняемой законом компьютерной информации (информации ограниченного доступа); последствие (альтернативно) в виде уничтожения, блокирования, модификации, копирования компьютерной информации, и причинно-следственную связь между указанным действием и любым из названных последствий.

Законодателем не уточнено понятие доступа к информации. Указанное понятие содержится в п. 6 ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ "Об

информации, информационных технологиях и о защите информации”: “доступ к информации – возможность получения информации и ее использования”.

Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.).

Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

Другими словами, неправомерный доступ к компьютерной информации – это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из последствий:

а) уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое “вытеснение” старых версий файлов последними по времени;

б) блокирование информации – результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации – внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) копирование информации – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Однако, по нашему мнению, если в силу настроек компьютерной программы при работе с ней, пусть даже и в результате неправомерного доступа,

автоматически создается резервная копия компьютерной информации, то данное действие не будет иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит.

Преступление окончено с момента наступления любого из указанных последствий. Устанавливая причинную связь между несанкционированным доступом и наступлением вредных последствий следует иметь в виду, что в компьютерных системах возможны уничтожение, блокирование и модификация компьютерной информации в результате технических неисправностей или ошибок при функционировании операционной среды или иных программ. В этих случаях лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности по данной статье ввиду отсутствия причинной связи между его действиями и наступившими последствиями.

Субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла (прямого или косвенного) или неосторожности.

Субъект преступления общий – вменяемое лицо, достигшее шестнадцати лет. Вместе с тем ч. 3 ст. 272 УК РФ предусматривает наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения.

Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие).

«Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»

Статья 273 УК РФ предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Компьютерная программа – это объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата.

Очевидно, что под компьютерными программами по смыслу данной статьи УК РФ в основном понимаются программы, известные как компьютерные вирусы (черви, троянские кони, кейлоггеры, руткиты и др.).

Основной объект преступления – общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Предмет преступления по содержанию совпадает с предметом преступления, предусмотренного ст. 272 УК РФ.

Объективная сторона преступления включает альтернативные действия, состоящие: а) в создании программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты; б) в распространении таких программ или машинных носителей с такими программами; в) в использовании таких программ или машинных носителей с ними.

Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением таких программ понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая продажу, прокат, бесплатную рассылку по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом.

Использование программы – это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме. Под использованием вредоносных программ понимается их применение (любым лицом), при котором активизируются их вредные свойства.

Рассматриваемое преступление будет окончено с момента создания, использования или распространения таких программ или информации, создающих угрозу наступления указанных в законе последствий, вне

зависимости от того, наступили реально эти последствия или нет. Состав преступления формальный.

Субъективная сторона состава преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется виной в виде прямого умысла. При этом виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к указанным в законе общественно опасным последствиям. Мотив и цель не влияют на квалификацию преступления.

Субъект преступления общий – вменяемое лицо, достигшее шестнадцати лет.

В ч. 3 ст. 273 УК РФ предусмотрен квалифицирующий признак рассматриваемого состава преступления – наступление тяжких последствий или создание угрозы их наступления. Следует учитывать, что в случае наступления тяжких последствий данный квалифицированный состав преступления является материальным, то есть деяние окончено с момента наступления общественно опасных последствий, а если создана угроза их наступления, то состав является усеченным.

При этом тяжесть последствий должна определяться с учетом всей совокупности обстоятельств дела (причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и др.).

Субъективная сторона указанного квалифицированного состава преступления характеризуется двумя формами вины – умыслом по отношению к самому деянию и неосторожностью по отношению к последствиям. В случае если преступник умышленно относился к наступлению тяжких последствий или созданию угрозы их наступления, то в зависимости от качественной и количественной оценки наступивших тяжких последствий его действия подлежат дополнительной квалификации по совокупности преступлений, предусмотренных соответствующими статьями УК РФ.

Следует иметь в виду, что ст. 273 УК РФ устанавливает ответственность за незаконные действия с компьютерными программами, записанными не только на машинных, но и на иных носителях, в том числе на бумаге. Это обусловлено тем, что процесс создания компьютерной программы зачастую начинается с написания ее текста с последующим введением его в компьютер или без такового. С учетом этого наличие исходных текстов вредоносных компьютерных программ уже является основанием для привлечения к ответственности по ст. 273 УК РФ. Однако использование вредоносной компьютерной программы для личных нужд (например, для уничтожения собственной компьютерной информации) ненаказуемо. В случае если действие вредоносной программы было условием совершения другого преступления, содеянное подлежит квалификации по совокупности преступлений вне зависимости от степени тяжести другого преступления.

Диспозиция части 1 статьи 273 УК РФ ранее была изложена следующим образом: “Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному

уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами" (в ред. от 08.12.2003). В действующей редакции от 07.12.2011 диспозиция ч. 1 ст. 273 УК РФ предусматривает ответственность за "создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации".

Гражданский кодекс Российской Федерации определяет программу для ЭВМ как "представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения".

«Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

В соответствии со ст. 274 УК РФ уголовная ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Диспозиция ч. 1 ст. 274 УК РФ ранее предусматривала ответственность за “нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред”. В редакции Федерального закона от 07.12.2011 N 420-ФЗ “О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации” она изложена следующим образом: “Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб”.

Основной объект преступления – общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Дополнительный объект преступления, повлекшего причинение существенного вреда, – общественные отношения, обеспечивающие в зависимости от характера последних, иные значимые социальные ценности (жизнь человека, здоровье многих людей, собственную безопасность и т.п.).

Предметом данного преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

Данная норма является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети Интернет, не существует.

Объективная сторона преступления состоит в нарушении правил хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если такое нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь, а также доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными ст. 272 и 273 УК РФ.

Правила, о которых идет речь в ст. 274 УК РФ, должны быть направлены только на обеспечение информационной безопасности. В ней говорится о нарушении правил, которое может повлечь уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, то есть такие же последствия, что и при неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных программ для ЭВМ.

Правила доступа и эксплуатации, относящиеся к обработке информации, содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах.

«Прокурорский надзор на стадии возбуждения уголовного дела о преступлениях в сфере компьютерной информации»

В последние годы, наиболее часто, возбуждение уголовных дел этой категории происходит по поводу, предусмотренному п. 3 ч. 1 ст. 140 УПК РФ, а именно по материалам, содержащим результаты оперативно-розыскных мероприятий специализированных подразделений МВД России и ФСБ России. В частности, для выявления преступлений в сфере так называемых высоких технологий (к которым относятся и преступления в сфере компьютерной информации), а также для установления лиц и преступных группировок, занимающихся преступной деятельностью в этой области, создано Управление “К” МВД России.

Вместе с тем, прокурору необходимо тщательно проверять законность возбуждения уголовных дел и оценивать представленные материалы.

Учитывая стремительное развитие компьютерных технологий, изобретательность и высокую квалификацию лиц, совершающих компьютерные преступления, охватить многообразие всех существующих способов совершения преступлений в сфере компьютерной информации не представляется возможным. Тем не менее, в данной работе следует указать наиболее распространенные из них.

Способы совершения преступления, предусмотренного ст. 272 УК РФ, можно разделить на две группы. К первой относятся способы непосредственного воздействия лица на компьютерную информацию, когда проникновение осуществляется путем введения различных команд в компьютерную систему. В этом случае следы совершения преступления останутся только на носителе компьютерной информации, задействованном при совершении преступного посягательства. Такой доступ может осуществляться как лицами, имеющими право на него, так и лицами, специально проникающими в зоны с ограничениями по допуску.

Вторая группа – это способы удаленного (опосредованного) воздействия на компьютерную информацию, например: проникновение в чужие информационные сети путем соединения с тем или иным компьютером; проникновение в компьютерную систему с использованием чужих идентификационных данных; подключение к линии связи легитимного пользователя с получением доступа к его системе; использование вредоносных программ для удаленного доступа к информации и т.п.

Способы совершения преступлений, предусмотренных ст. 273 и 274 УК РФ, в достаточной степени описаны в главе первой настоящих рекомендаций при рассмотрении объективной стороны указанных составов преступлений.

«Установлен механизм самоограничения прав на участие в азартных играх»

С 1 сентября 2026 года (за исключением положения, для которого установлен иной срок вступления в силу) вступает в силу Федеральный закон от 29.12.2025 № 575-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», устанавливающий механизм самоограничения прав на участие в азартных играх.

Физическое лицо вправе отказаться от участия в азартных играх путём направления в единый регулятор азартных игр заявления о включении информации о физическом лице в перечень физических лиц, отказавшихся от участия в азартных играх.

Единый регулятор азартных игр ведёт перечень физических лиц, отказавшихся от участия в азартных играх.

Не допускается направление рекламы организаторами азартных игр, а также третьими лицами, действующими по поручению или в интересах организаторов азартных игр, в адрес физического лица, информация о котором включена в перечень физических лиц, отказавшихся от участия в азартных играх.

«Увеличен размер исполнительского сбора и уточнен порядок его взимания»

Федеральным законом от 29.12.2025 № 563-ФЗ в Федеральный закон «Об исполнительном производстве» внесено изменение, согласно которому исполнительский сбор устанавливается в размере 12% от подлежащей взысканию суммы или стоимости взыскиваемого имущества (ранее – 7%). Минимальный размер сбора увеличен в два раза - 2 тысячи рублей с физического лица (в том числе с индивидуального предпринимателя) и 20 тысяч рублей с должника – организации.

В случае неисполнения исполнительного документа неимущественного характера исполнительский сбор также увеличивается в два раза - до 10 тысяч и 100 тысяч рублей соответственно.

Кроме того, введено положение, устанавливающее порядок взимания и размер сбора в случае неисполнения должником исполнительного документа имущественного характера, а также уточнен порядок распределения денежных средств, поступивших на депозитный счет службы судебных приставов при исполнении требований имущественного характера.

«Принят новый порядок предоставления сведений о доходах, об имуществе и обязательствах имущественного характера»

Принят новый порядок предоставления сведений о доходах, об имуществе и обязательствах имущественного характера.

Изменения затронули, в частности, государственных (муниципальных) служащих, судей, сотрудников некоторых правоохранительных органов, Банка России, Счетной палаты, лиц, занимающих должности в госкорпорациях (компаниях), государственных внебюджетных фондах, атаманов казачьих обществ и др.

Так, Федеральным законом от 28.12.2025 № 505-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» внесены поправки в ряд законодательных актов и предусматривают, в частности: представление сведений о доходах, имуществе и обязательствах имущественного характера, предусмотренных Федеральным законом «О противодействии коррупции», только претендентами на должности; представление действующими сотрудниками сведений о расходах, предусмотренных Федеральным законом «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам», в установленных законом случаях. Данные сведения необходимо будет представить не позднее 30 апреля года, следующего за годом, в котором возникли такие основания.

Также законом отменены положения, устанавливающие требование о размещении представленных сведений в сети Интернет. Указанный Федеральный закон вступил в силу 1 января 2026 года.

«С 1 марта 2026 г. устанавливается порядок уничтожения метанола и метанолсодержащих жидкостей»

Постановлением Правительства РФ от 29.11.2025 № 1965 «Об утверждении Правил уничтожения метанола и метанолсодержащих жидкостей» с 1 марта 2026 г. устанавливается порядок уничтожения метанола и метанолсодержащих жидкостей.

Метанол и метанолсодержащие жидкости уничтожаются с соблюдением требований санитарных правил СП 2.2.5.4116-25 «Санитарно-эпидемиологические требования к организации и проведению работ с метанолом», утвержденных постановлением Главного государственного санитарного врача Российской Федерации от 27 марта 2025 г. № 7, и межгосударственного стандарта ГОСТ 2222-95 «Метанол технический. Технические условия», введенного в действие постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 22 марта 2000 г. № 60-ст с 1 января 2001 г.

При уничтожении применяются термический, биологический и иные способы уничтожения метанола и метанолсодержащих жидкостей в соответствии с межгосударственным стандартом ГОСТ 2222-95 «Метанол технический. Технические условия», введенным в действие постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 22 марта 2000 г. № 60-ст с 1 января 2001 г.

Организация или индивидуальный предприниматель обязаны вести учет уничтоженных метанола и метанолсодержащих жидкостей. В день уничтожения составляется акт, в котором указываются объем (количество), дата, место и способ уничтожения метанола и метанолсодержащих жидкостей. Акт подписывается ответственными должностными лицами организаций или индивидуальными предпринимателями.

Настоящее Постановление действует до 1 марта 2032 г.

«Уточнен порядок включения в страховой стаж периодов ухода за детьми до 1,5 лет»

Постановлением Правительства РФ от 19.01.2026 №11 «О внесении изменений в некоторые акты Правительства Российской Федерации» уточнены порядок включения в страховой стаж периодов ухода за детьми до 1,5 лет, а также правила исчисления «сельского» стажа, дающего право на повышение фиксированной выплаты к страховой пенсии.

Согласно внесенным поправкам в страховой стаж одному из родителей засчитываются периоды ухода за каждым ребенком до 1,5 лет без верхнего ограничения, предусмотренного ранее (не более 6 лет в общей сложности). Кроме того, в случае многоплодной беременности периоды ухода одного из родителей за каждым ребенком до 1,5 лет теперь должны суммироваться с учетом их фактической продолжительности.

Также внесены уточнения в правила исчисления периодов работы в сельском хозяйстве, дающей право на надбавку к фиксированной выплате при назначении пенсии (исключено условие о том, что надбавка устанавливается только на период проживания в сельской местности, а также исключено ограничение «не более 6 лет» в части периодов ухода за детьми).

Действие постановления распространяется на правоотношения, возникшие с 1 января 2026 г.

«Студенческие билеты и зачетные книжки для обучающихся в вузах переводятся в электронный формат»

На основании Федерального закона от 29.12.2025 №539-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» студенческие билеты и зачетные книжки для обучающихся в вузах переводятся в электронный формат.

В Законе об образовании закреплено, что студенты вузов и научных организаций, ординаторы, ассистенты-стажеры и аспиранты получают сведения о студенческих билетах, сведения об иных документах, подтверждающих обучение по программам ординатуры, ассистентуры-стажировки, программам подготовки научных и научно-педагогических кадров в аспирантуре, в электронном виде в электронной информационно-образовательной среде организации, в которой они получают образование, через Единый портал госуслуг, а также с использованием многофункционального сервиса обмена информацией (мессенджера MAX).

Сведения о зачетных книжках предоставляются обучающимся в электронном виде в электронной информационно-образовательной среде образовательной организации и на Едином портале госуслуг. Предусмотрено, что по заявлению студента вышеназванные документы можно будет получить в вузе на бумажном носителе.

В вузах, подведомственных силовым структурам, студенческие билеты и зачетные книжки будут выдаваться только на бумажном носителе. Также для студентов закреплена возможность предъявления электронного студенческого билета для подтверждения обучения с использованием мессенджера MAX.

Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

«Административная ответственность за нарушение заказчиком срока оплаты товаров, работ»

Федеральным законом от 29.12.2025 №524-ФЗ «О внесении изменения в статью 7.30.4 Кодекса Российской Федерации об административных правонарушениях» установлена административная ответственность за нарушение заказчиком срока оплаты товаров, работ, услуг по договору (отдельному этапу договора), заключенному по результатам закупки, будет наступать вне зависимости от наличия у поставщика (подрядчика, исполнителя) статуса субъекта малого или среднего предпринимательства.

«Увеличены размеры административных штрафов за нарушение требований к перевозке детей»

Федеральным законом от 29.12.2025 № 525-ФЗ "О внесении изменений в статью 12.23 Кодекса Российской Федерации об административных правонарушениях" увеличены размеры административных штрафов за нарушение требований к перевозке детей, установленных Правилами дорожного движения, налагаемых на водителя, на должностных лиц и на юридических лиц.

Речь идёт о двукратном увеличении штрафов за отсутствие автокресла, его несоответствие требованиям закона или другие нарушения правил перевозки детей:

штраф увеличен с 3 000 до 5 000 рублей - для водителей;

штраф увеличен с 25 000 до 50 000 рублей - для должностных лиц, а также самозанятых водителей такси;

штраф увеличен со 100 000 до 200 000 рублей - для ИП и юридических лиц.